POLICE DEPARTMENT'S TRACKING EFFORTS BASED ON FALSE STATISTICS

Thu 26 May 2016
By Freenet Project Inc.

Documents initially made public by the Missouri police department describe their efforts on tracking Freenet usage. Using a simple scheme, they claim a near zero false positive rate for tracking the originator of a download. While we applaud all public documentation on attacks, we have to point out that the claimed effectiveness of their attacks is based solely on flawed mathematics. In reality, the false positive rate of their method is at least 83%, and close to 100% in real world scenarios.

The claimed effectiveness of their attack is based on a false assumption about the distribution of the HTL of incoming requests. HTL (Hops to Live) is a number embedded in each request that is usually decremented when the request is forwarded, starting at a value of 18 at the originator of the request, and serves to limit the number of hops a request can survive on the network. As a security precaution, the HTL is decremented probabilistically on the first few hops. In their tracking efforts, the Missouri police department assumes that when multiple requests for pieces of a file arrive from a single

requests (not only a single one, as would be the case with per-request probabilistic decrementing) did not originate from the node from which we received them but were forwarded one step. So for 10 connections (the lowest number of peers Freenet uses), there are on average 5 other nodes whose HTL 18 requests are forwarded with HTL 18, so the probability that a given HTL 18 request originated at the node from which we received it is only about 17% (1 in 6). If the node has more connections (close to 30 is common), this probability is even lower. And this probability does not get higher when gathering more requests of chunks from a specific file or a specific kind of files, because they can reasonably all be forwarded from a different node — the one which really sent them.

The heterogenity of the network and routing with second-level connections taken into account does not easily yield robust statistical claims without knowing the peers of peers of the node under investigation. Staying connected for a long time might allow for distinguishing between the changing peers of the node and requests originating at the node itself, but with significant cost.

If the node which is tracked has friend-to-friend peers (which unlike automatically added peers do not change regularly), even waiting will not allow finding out with the described method whether HTL 18 requests came from the node itself or from the peers connected over friend-to-friend connections.

For details, see the code.

This does not make it impossible to track Freenet users who use only Opennet mode (connecting to strangers), since a network where nodes connect to strangers is inherently susceptible to Sybil attacks, where nodes of typical users are outnumbered by malicious, colluding nodes.

The only way to defend against serious attacks is to *use Freenet in Friend-to-Friend mode*, where the precondition to tracking a user is social engineering to get the people to whom he/she is connected to betray the user. The need to defend against this type of attack is the reason why the core of Freenet was rewritten in 2007 to add this Friend-to-Friend mode (called Darknet mode).

However the method used by the Missouri police department is using false statistics: despite its flaws, Freenet's Opennet is much harder to track than they claim.

The Freenet developers do not condone these attacks. Police departments try to use every legal venue to catch criminals. This is their job and vocation, but any attack they find could also be used by oppressive governments to suppress dissenting opinions, so we will work to fix attacks as they come to light. We expect law enforcement to get their math right, especially when using it in court. If they can get a warrant with an 83% false positive rate, that's a problem for lawmakers. If they falsely claim a 0% false positive rate, that's eroding the trust of citizens in the legal system.

Additional information on this attack is available from the mailing list discussion.

The mission of the Freenet Project is to safeguard freedom of the press by providing censorship resistant communication. This requires protecting people against being targeted for what they write or read. To achieve this, Freenet enables users to publish anonymous websites and offers chat, forums, and file-sharing, as well as confidential communication among friends and methods to leverage the capabilities of Freenet from other tools.

When the police spread misinformation about the security of Freenet, it directly undermines our mission by driving users to networks which cannot provide a comparable level of security for whistle-blowers and those wishing to publish anonymously.

News Archives